

IMPACTO DEL RIESGO CIBERNÉTICO EN EL SEGMENTO MIPYME.

Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme

Sara Villa Mesa

Trabajo de Grado para Optar al Título de Magíster en Economía Aplicada

Asesores: Ph.D Alvaro Hurtado Rendón

MBA. Andrés Mejía Mejía

Universidad EAFIT

Programa de Maestría en Economía Aplicada

Medellín

2018

Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme.

Por: Sara Villa Mesa

Resumen

El propósito de este trabajo es analizar el impacto del seguro de riesgo cibernético en la protección de las utilidades para el segmento Mipyme en Colombia, mediante el estudio de un grupo de empresas pertenecientes al segmento, las cuales experimentaron pérdidas debido a incidentes cibernéticos. Para el cálculo de la Utilidad Esperada EU, se utiliza la función de aversión al riesgo CRRA. Donde a partir del análisis de datos de 50 empresas afectadas, se comprueba como el seguro es un mecanismo de transferencia de riesgo que apalanca el bienestar de las empresas Mipyme.

Palabras claves: *Riesgo cibernético, seguros, ciberseguridad, crimen cibernético, seguridad de la información, bienestar.*

Abstract

The main purpose of this work is to analyze the impact of cyber risk insurance on the protection of profits for the Mipyme segment in Colombia, by studying a group of companies belonging to the segment, which experienced losses due to cyber incidents. For the calculation of the expected utility EU, the risk aversion function CRRA is used. Where from the analysis of data of 50 affected companies, it is verified how the insurance is a risk transfer mechanism that improve the wealth of the Mipyme companies.

Palabras claves: *cyber risk, insurance, cybersecurity, cybercrime, IT security, wealth.*

Tabla de contenido.

Introducción	1
Descripción del problema	2
Objetivo general.....	6
Objetivos específicos	6
Marco Teórico.....	7
Antecedentes	9
Caracterización del segmento Mipyme.....	13
El riesgo cibernético, su impacto en las Mipymes y el seguro.	14
El cibercrimen en Colombia y en sus empresas.....	16
Seguros de riesgo cibernético en Colombia para empresas:	18
Cálculo del impacto del crimen cibernético en las Mipymes.	18
Análisis y proyección de resultados:.....	27
Ejercicio exploratorio de proyección de resultados y análisis del PIB	28
Conclusiones	31
Referencias.....	32
Anexo 1	35
Anexo 2.....	37
Anexo 3.....	40

Introducción

El riesgo cibernético para cualquier organización se refiere a los riesgos asociados a las vulnerabilidades de los sistemas tecnológicos, que amenazan la disponibilidad, integridad y/o confidencialidad de la información almacenada en medios digitales. Este riesgo a su vez, expone a una empresa a experimentar pérdidas financieras e interrupciones totales o parciales de sus operaciones, esto debido a la materialización de un evento donde se vea afectada su información. (Eling & Schnell, 2016).

Teniendo en cuenta el panorama empresarial colombiano, donde las Mipymes según publicación de la Banca de Oportunidades (2017) son el 73% de las empresas en Colombia, es relevante para el segmento, conocer, comprender y aprender a prevenir y gestionar el riesgo cibernético, dado que de llegar a materializarse podría generarse una cadena de eventos desafortunados que ponen a prueba su supervivencia como: exposición de la reputación, pérdidas financieras, pérdidas de clientes e incluso la desaparición de su negocio (Allianz Global Corporate & Specialty SE, 2018). Este proyecto de grado, pretende entonces calcular los impactos en el bienestar de las Mipymes cuando han sufrido algún tipo de crimen cibernético y como el seguro se convierte en una herramienta efectiva de transferencia del riesgo y protección de las utilidades de la empresa.

Descripción del problema

El internet, que permite una gran velocidad en las comunicaciones, el acceso a la información global y el aumento del valor de los activos de información digital para las personas y para las empresas, ha hecho posible una nueva forma de hacer negocios, donde la digitalización de los procesos y la información son protagonistas. Esta revolución de la información, trae consigo una serie de desafíos pues la inmediatez con la que se están creando continuamente avances tecnológicos hacen que junto con las oportunidades aparezcan también los riesgos y amenazas. Uno de los riesgos más relevantes es el riesgo cibernético, el cual se presenta como una de las mayores amenazas a los activos intangibles más importantes para una empresa, como lo es la información.

El riesgo cibernético es un riesgo de carácter operacional y sin fronteras definidas. Puede comprenderse como aquel peligro o amenaza que surge al usar sistemas tecnológicos interconectados y se materializa cuando se produce una afectación a uno o varios de los tres atributos de la información, definidos como (Christian Biener, 2015):

La confidencialidad: hace referencia a la protección de la información para que no sea compartida no divulgada sin autorización de su dueño.

La Integridad: significa que los datos guardados en internet deben permanecer tal y como fueron almacenados por su dueño, no deben ser vulnerados ni modificados por terceros.

La Disponibilidad: quiere decir que la información debe permanecer disponible en todo momento para su dueño y se le debe permitir el acceso en el momento en que la necesite.

La alta dependencia del internet para hacer negocios genera una nueva dinámica económica para el sector empresarial, donde estar conectado se hace vital para el desarrollo de cualquier empresa y la exposición a un evento cibernético se convierte en un asunto de gran

preocupación para las mismas, tanto así que el riesgo cibernético hoy es catalogado como uno de los riesgos de mayor preocupación a nivel mundial. AON Compañía multinacional de corretaje de seguros y reaseguro en su reporte anual de riesgos, ubica el riesgo cibernético en el quinto puesto entre los riesgos más relevantes a nivel mundial , escalando 4 puestos desde 2015 (AON Risk Solutions, 2017). Este riesgo es también mencionado por el “Global Risk Report” como uno de los desafíos crecientes de mayor preocupación por parte del gobierno y la industria en diferentes países (World Economic Forum, 2018).

Si bien de este riesgo se viene hablando hace ya varios años, durante el 2017 se han presentado varios casos. El más relevante es el de “Wanna Cry”¹, ataque cibernético mediante ransomware (secuestro de información) donde de acuerdo al artículo “Europe Economy: WannaCry Ransomware” (The Economist Intelligence Unit, 2017) se presentó el secuestro de información en aproximadamente 300.000 equipos conectados a internet y su ámbito territorial abarco alrededor de 150 países. Este caso entre otros, ha permitido que crezca la preocupación a nivel mundial por crear capacidades de reacción y protección para este riesgo operacional de carácter sistémico, debido a su gran capacidad de propagación.

Teniendo en cuenta que el gran dinamizador de la economía colombiana son las empresas, cuando se habla de la materialización del riesgo cibernético para una empresa, se refiere a que esta enfrenta situaciones relacionadas con crímenes digitales, donde la información y los sistemas tecnológicos se ven comprometidos y como consecuencia de esto puede generarse la interrupción del negocio y en algunos casos la pérdida o secuestro de la información, la cual es catalogada como uno de los activos más importantes para una empresa, tanto así que la

¹ Uno de los peores ataques cibernéticos de ransomware en la historia

empresa de AON Company, STROZ FRIEDBER² indica en uno de sus estudios que la información de una empresa es valorada como un activo 14% más valioso que los activos tangibles como las propiedades. Esta situación pone en peligro la capacidad de permanencia en el mercado de una empresa, pues compromete no solo su operación si no también su reputación y su capacidad de recuperarse, seguir generando empleo y aportando al PIB del país. Para el caso de las Mipymes es aún más complejo, pues el tener que enfrentarse a una situación de estas, podría ser un desafío mayor, ya que de acuerdo a sus características es muy probable que no tenga la capacidad de recuperarse en caso de sufrir un evento cibernético de alto impacto.

El Segmento Mipyme como su nombre lo indica lo conforman las micro, pequeña y mediana empresa, las cuales según el Ministerio de Comercio Industria y Turismo de Colombia son alrededor de 2.5 Millones y son responsables de alrededor del 28% del PIB colombiano. (ACOPI, 2018) . Estos datos, ratifican la importancia que representa para la economía del país. Siendo así, es relevante conocer el efecto que puede llegar a tener el crimen cibernético en términos de afectación de las utilidades e interrupción de las operaciones de las Mipymes.

Las Mipymes suelen ser un blanco fácil para los delincuentes cibernéticos, pues debido a sus características de supervivencia no logran enfocar sus esfuerzos en la protección tecnológica y la seguridad cibernética, por lo tanto, no están preparadas para gestionar este riesgo. A esto se suma que la cifra de acceso al mercado de seguros por parte del segmento, según Fasecolda es de solo alrededor del 5% (Fasecolda, Federación de aseguradores colombianos 2017), lo cual confirma que dentro de sus prioridades principales no está el aseguramiento. Estos datos son alarmantes, principalmente porque en el último informe de crimen cibernético de la policía

² Según infografico de riesgo cibernético de STROZ FRIEDBER an AON Company

nacional, se indica que los ataques cibernéticos han ido migrando de personas a empresas (Centro Cibernético Policial, 2017).

El segmento Mipyme aún desconoce las consecuencias que puede llegar a tener al enfrentarse un evento cibernético y se presenta incertidumbre alrededor de los impactos financieros y los efectos que puede acarrearles. Este trabajo de grado pretende responder a la siguiente pregunta: ¿Puede el seguro de riesgo cibernético apalancar el bienestar de las Mipymes en Colombia, mediante la protección de sus utilidades cuando son víctimas de crímenes cibernéticos? Mediante esta respuesta se busca entregarle al empresario Mipyme y al sector asegurador un panorama en diferentes escenarios, donde se revisará si la adquisición de un seguro juega un papel importante en la generación de bienestar en términos de protección de las utilidades y la capacidad de resiliencia para que la Mipyme permanezca en el mercado.

Objetivo general

Encontrar la relación entre el seguro de riesgo cibernético y el bienestar en términos de utilidades para el segmento Mipyme en Colombia por medio de un análisis cuantitativo del seguro como herramienta de transferencia del riesgo y protección de la utilidad.

Objetivos específicos

- Caracterizar el segmento Mipyme en Colombia con el fin de entender cuál es la penetración de los seguros y su exposición frente al riesgo cibernético.
- Entender el riesgo cibernético, sus manifestaciones y sus propiedades, así mismo conectar este estudio con las posibles afectaciones al sector Mipyme en Colombia, de acuerdo con sus características.
- Encontrar el impacto de la materialización del riesgo cibernético en las utilidades de 50 Mipymes en términos de las posibles pérdidas.

Marco Teórico

Las cámaras de comercio de cada una de las regiones, el Ministerio de Comercio, Industria y Turismo de Colombia, y las corporaciones como iNNpulsa³, Parque del Emprendimiento⁴, Créame⁵ entre otros, son entidades por medio de las cuales Colombia ha concentrado sus esfuerzos en los últimos años en incentivar los emprendimientos y fomentar la innovación y la creación de empresa, debido a esto el segmento Mipyme viene creciendo y convirtiéndose en un sector estratégico de la economía colombiana. Esta situación trae consigo desafíos para el sector financiero y asegurador de crear productos masivos pero personalizados para las Mipymes. De este modo las aseguradoras se están reinventando y produciendo soluciones escalables de gestión y transferencia de riesgo para el segmento, con el fin de identificar su nivel de aversión al riesgo y de acuerdo con esto entregarles esa capacidad de resiliencia que puede aportar un seguro.

El seguro ha sido tradicionalmente un mecanismo de transferencia del riesgo, que le permite a las empresas asumir solo la porción del riesgo que desea y están en capacidad de asumir de acuerdo a su realidad. Históricamente el seguro ha sido adquirido para proteger riesgos de las propiedades como incendios o terremotos al igual que la responsabilidad por daños a terceros, es decir, el aseguramiento ha estado enfocado en el respaldo de daños o perjuicios evidentes. Con la aparición de el crimen cibernético, las aseguradoras deben replantearse la forma como han creado las soluciones de aseguramiento hasta hoy, teniendo en cuenta que las

³ iNNpulsa Colombia: “Unidad de Gestión de Crecimiento Empresarial del Gobierno Nacional, creada en febrero de 2012 para promover el emprendimiento, la innovación y la productividad como ejes para el desarrollo empresarial y la competitividad de Colombia”. tomado de <https://www.innpuolombia.com/es/nuestra-organizacion> (2018)

⁴ Parque del Emprendimiento: “plataforma especializada en emprendimiento, dedicada a fomentar la cultura emprendedora y a fortalecer iniciativas y proyectos empresariales innovadores, que dinamizan la economía de la región y que se proyectan hacia mercados nacionales e internacionales”. Tomado de <http://parquedeemprendimiento.com/quienes-somos/> (2018)

⁵ Créame:” incubadora y aceleradora que promueve servicios que maximizan el valor empresarial, a través de modelos de negocio de acuerdo a las necesidades de los clientes, dinamizando oportunidades, convirtiéndonos en su aliado estratégico en programas de Responsabilidad Social Empresarial y Desarrollo Empresarial”. Tomado de https://www.cream.com.co/index.php?option=com_content&view=article&id=141&Itemid=313 (2018)

consecuencias que acarrea a los negocios son de dimensiones diferentes y de mayor incertidumbre en la cuantificación de posibles pérdidas futuras.

El seguro en general tiene una función de gran importancia para el sector económico y es garantizar esa capacidad de resiliencia, que en el segmento Mipyme puede llegar a convertirse en una capacidad de supervivencia. De acuerdo al artículo de Kuru y Bayraktar (2017), el seguro contra el riesgo cibernético es una inversión con altos índices de seguridad que, junto con una estructura robusta de protección tecnológica, tiene un impacto positivo para protección de las utilidades y así mismo en la generación de bienestar, afirmación que se pretende comprobar mediante este trabajo.

En el artículo de referencia se usó una metodología en la cual se usa la función de utilidad de Von-Neumann y Morgenstern donde se plantea un modelo probabilístico simple para analizar la decisión o no de compra del seguro. Adicionalmente se tienen en cuenta otros factores importantes como la aversión al riesgo de los compradores y las probabilidades de ocurrencia de un crimen cibernético. El ámbito analizado en el artículo de referencia se limita a la aplicación en 3 países, Estados Unidos, Reino Unido y Turquía, donde se puede ver como la utilidad es cambiante de acuerdo a los diferentes escenarios que presentan en relación a la aversión al riesgo, a los países analizados, las probabilidades de ocurrencia de los ataques cibernéticos, las preferencias de compra del seguro y las primas cobradas. Los resultados se relacionan con el PIB de cada uno de los países seleccionados, determinando cuales son lo más vulnerables a la afectación de las utilidades. A partir de esta información se analizaron los problemas que debe enfrentar el sector asegurador con respecto al costo de las primas y la gestión del riesgo.

Para efectos de este trabajo se revisará si el modelo utilizado se adapta a la información recolectada, con el fin de encontrar respuestas que representen de manera más fiel la realidad del

segmento. Finalmente, se pretende comprobar que el seguro de riesgo cibernético aumenta el bienestar de una empresa del segmento analizado en Colombia y así mismo, aportar a la continuidad y crecimiento de este segmento de la economía colombiana que a su vez se traduce en crecimiento económico para el país debido a lo que representa en términos de aporte al PIB y a la generación de empleo.

Antecedentes

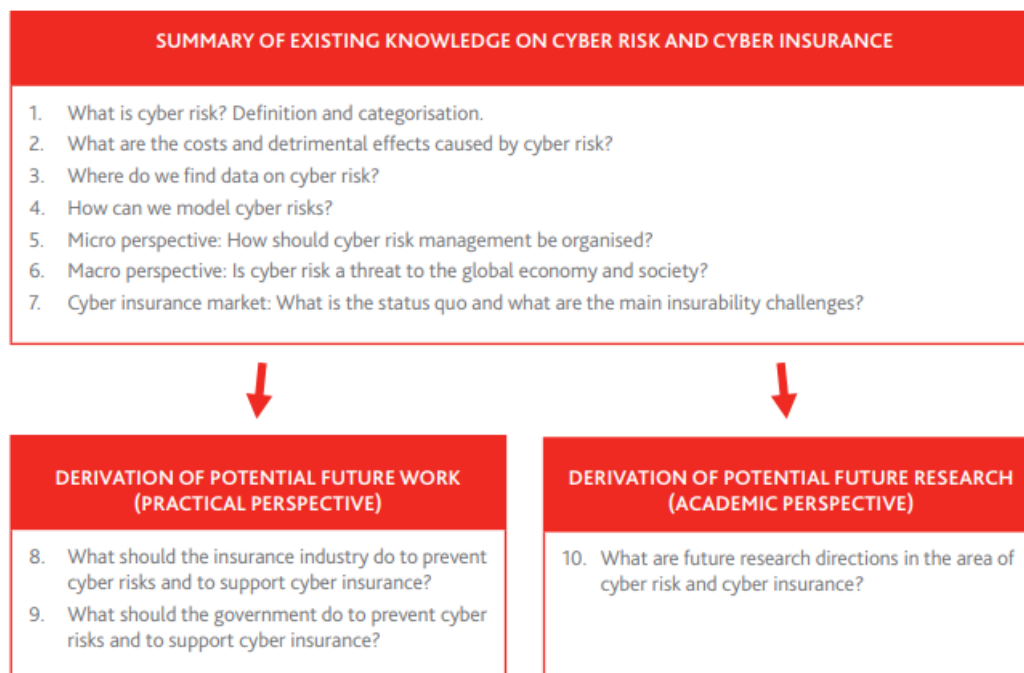
En los últimos 3 años, el riesgo cibernético y su impacto en los diferentes sectores de la economía se hace cada vez más común y crece la preocupación por los impactos que aún pueden ser inesperados. A raíz de esto surgen diferentes análisis y acercamientos al entendimiento del riesgo. Estos análisis van desde los impactos en la industria hasta tratar el tema como un asunto gubernamental y de políticas públicas.

El riesgo cibernético es catalogado por Guy Carpenter⁶ como uno de los riesgos emergentes de impacto público y de prioridad estratégica para la industria y los gobiernos alrededor del mundo (Guy Carpenter & Company, LLC, 2015). A partir de este informe, se menciona que el alcance destructivo del riesgo cibernético para todo tipo de industrias aun es desconocido y en esto radica la mayor preocupación, pues esto hace que sea difícil aproximarse a la gestión de este, pues los daños que puede acarrear superan el ciberespacio ingresando a la vida real con la capacidad de producir pérdidas físicas como consecuencia de ataques a los sistemas tecnológicos. Guy Carpenter, realiza un análisis del riesgo desde los negocios y su exposición,

⁶ “Corredor de Reaseguros que hace parte del grupo Marsh & McLennan, fue fundado en 1921 tiene operaciones en más de 50 países. Se caracteriza por ser uno de los brokers más grandes del mundo, líder en lograr soluciones integrales para la industria aseguradora, mediante una robusta combinación de experiencia en el corretaje, servicios de consultoría, investigación y análisis estratégico”. (Fasecolda, 2018)

donde explica la taxonomía del riesgo cibernético para las corporaciones, para esto realiza un mapa de los actores y los campos de ataque para luego analizar los posibles daños causados desde todos los ángulos.

Posteriormente en 2016 The Geneva Association publica un informe sobre el conocimiento actual del riesgo cibernético. Dicho informe es interesante pues la aproximación al riesgo se realiza a partir de 10 preguntas y sus respectivas respuestas de acuerdo a un análisis de las definiciones en la industria aseguradora para luego discutir estos resultados con los expertos internos y posteriormente comparar la información recolectada con 211 artículos académicos de carácter empíricos, teóricos y cuantitativos, para lo cual se revisaron publicaciones entre el año 2000 y 2015 de revistas como *Journal of Finance*, *American Economic Review*, *Journal of Risk and Insurance*, *Insurance: Mathematics and Economics*, *The Geneva Papers on Risk and Insurance—Issues and Practice*, and *The Geneva Risk and Insurance Review*. Otras revistas académicas relacionadas con riesgos y seguros también fueron revisadas como (*Journal of Insurance Regulation*, *Risk Management & Insurance Review*, *ASTIN Bulletin*, *North American Actuarial Journal*, *European Actuarial Journal*). Este informe tiene como objetivo la generación de referencias literarias y académicas sobre los estudios, artículos, documentos de trabajo entre otros, que se han realizado sobre el riesgo cibernético y el seguro, con el fin de generar al sector una visión del ecosistema que permita un direccionamiento para la discusión y toma de decisiones sobre el aseguramiento de este riesgo, es por esto que el análisis se enfoca en responder las 10 preguntas claves que se definen en la figura 1.

Figura 1: Preguntas claves a responder

Fuente: The Geneva Association (Martin Eling, 2016)

Adicionalmente existen otros escritos e investigaciones aplicadas del sector asegurador que han sido desarrollados con el fin de entregar un entendimiento del riesgo cibernético y la importancia de este, como los documentos de riesgo cibernético del global risk center de Marsh and McLennan⁷ (compañía multinacional corredora de seguros), y el estudio de cibernético con relación a la segmentación del sector Mipyme en Colombia por Seguros Sura Colombia (2017).

Para determinar los impactos económicos que ha dejado históricamente los eventos cibernéticos, las compañías de AON Risk Solutions y sus compañías aliadas han hecho grandes esfuerzos por cuantificar las pérdidas asociadas en varias regiones y países como Europa, Medio Oriente, África, Estados Unidos, entre otros, donde fueron encontrados datos claves como por

⁷ Marsh and Mc McLennan, grupo de compañías del sector asegurador y compañía colaboradora del global risk report que publica World Economic Fórum.

ejemplo, para la región EMEA (Europa, Medio Oriente y África) en 2017 solo el 15% de las potenciales pérdidas de información están aseguradas y solo un 60% de los activos físicos que son susceptibles a sufrir daños derivados de un evento cibernético. Un 38% de las compañías en la región han sufrido pérdidas en los últimos 2 años por un aproximado de USD \$3.3 Millones, así mismo el 65% de las empresas esperan que las pérdidas asociadas al riesgo cibernético incrementen en los próximos 2 años (Ponemon Institute LLC & AON, 2017).

También es importante mencionar que firmas de consultoría en riesgos como Deloitte tienen artículos de gran valor con respecto a la gestión del riesgo cibernético y cuenta con un portal web⁸ donde se presentan una serie de artículos e información relacionados y de gran valor para el entendimiento del manejo del riesgo.

Pasando de un referenciación sectorial a una más académica, se han escrito artículos representativos acerca de la importancia del riesgo cibernético en el mundo. Shackelford (2017), plantea que los hacedores de políticas, deben considerar el riesgo cibernético como una de las amenazas más grandes en términos de seguridad y bienestar, no solo para los negocios sino también para cada uno de los ciudadanos, de modo que los sectores educativos, los juristas y los negociadores gubernamentales hagan énfasis en desarrollar leyes claras para regular las responsabilidades asociadas a las amenazas de la información (Shackelford, 2017) . Lo anterior muestra la importancia que toma este riesgo para la sociedad y la seguridad nacional de los países.

⁸ Portal cyber risk deloitte <https://www2.deloitte.com/ar/es/pages/risk/solutions/cyber-risk.html>

Caracterización del segmento Mipyme

El segmento Mipyme en Colombia está conformado por alrededor de 2.5 millones de empresas y son responsables según ACOPI, entre el 65% y 67% de los empleos formales (2017). El segmento empresarial colombiano está clasificado dentro de la Ley 590 de 2000 conocida también como la Ley Mipymes y modificada en la Ley 905 de 2004⁹, esta clasificación varía según sus activos totales en salarios mínimos mensuales legales vigentes (SMMLV)¹⁰ tal y como se muestra en la tabla 1.

Tabla 1: Clasificación empresarial colombiana.

Clasificación	Rangos (SMMLV)	Rango en Pesos Colombianos (COP)
Microempresa	0 – 500	\$0 - \$390.621.000
Pequeña	500 – 5000	\$390.621.000- \$3.906.210.000
Mediana	5000 – 30.000	\$3.906.210.000 - \$23.437.260.000
Grande	Superior a 30000	Superior a \$23.437.260.000

Fuente: elaboración propia basado en Ley 905 de 2004

El Sector Mipyme como su nombre lo indica lo conforman las micro, pequeñas y medianas empresas y dentro de estas tres, se encuentra la muestra utilizada para este estudio.

Esta clasificación, además de dividir las empresas por características cuantitativas, podría indicar por su tamaño, momentos económicos diferentes, distintas preferencias por el riesgo y

⁹ Tomado de Bancoldex. <https://www.bancoldex.com/Sobre-microempresas/Clasificacion-de-empresas-en-Colombia315.aspx>,

¹⁰ El Salario mínimos mensual legal vigente en Colombia para el 2018 es \$781.242

sus decisiones económicas y estratégicas | ser diversas según el pensamiento de sus directivos o creadores.

De acuerdo con lo anterior, es de gran importancia tener en cuenta el tamaño de la empresa y el nivel de aversión al riesgo para el análisis de utilidades ganadas debido al aseguramiento, además de la cantidad de cobertura comprada para transferir el riesgo cibernético.

Según el Ministerio de Comercio, Industria y Turismo en el año 2016 las Mipymes representaban el 99.9% de los establecimientos productivos, contribuían con el 80% del empleo y aportan el 40% del Producto Interno Bruto nacional, lo cual, si es comparado con las últimas cifras de ACOPI, ha disminuido considerablemente para el año 2017, ya que el aporte al PIB para este año se sitúa en el 28%. La dinámica del 2016 puede deberse a que según Confecámaras, ese mismo año creció en un 70,8% la creación de empresas en el país.

El riesgo cibernético, su impacto en las Mipymes y el seguro.

Lo que diferencia al riesgo cibernético de los otros riesgos es básicamente su territorio de aplicación, pues los riesgos cibernéticos ocurren en el ciberespacio¹¹, y además se propagan por las redes conectadas a internet (Eling & Schnell, 2016), a una velocidad nunca antes vista, lo que hace que sea un riesgo de características volátiles, sin fronteras definidas e intangibles, para el cual las pérdidas suelen ser de difícil cuantificación. El riesgo cibernético es un riesgo de carácter estratégico y operacional para las compañías, que afecta su operación en el momento en que la información se ve vulnerada en su confidencialidad, integridad y disponibilidad.

¹¹ El ciberespacio, describe cualquier red de servicio que se encuentre conectada a un sistema tecnológico. (Eling & Schnell, 2016)

Todas las empresas que se encuentren conectadas a internet, ya sea solo mediante un portal virtual bancario hasta una gran red de servidores, son propensas a sufrir un ataque cibernético. Es por esto que las compañías aseguradoras se han dado a la tarea de estudiar, comprender y cuantificar este riesgo, con el fin de entregar a las empresas y a las personas soluciones de aseguramiento que les permitan transferir esta exposición. Las Mipymes al ser un segmento importante del país e invertir de forma insuficiente en sus sistemas de protección digital y seguridad de la información, se convierten en un blanco fácil, pues los avances tecnológicos continuos acarrearán más peligros cibernéticos. Aun así, sus esfuerzos están enfocados en priorizar otro tipo de inversiones, pues de acuerdo con la “*Encuesta de desarrollo empresarial*” (ACOPI, 2018), solo el 32% de las Mipyme realizó alguna inversión durante el 2017 y estas fueron destinadas en un 32% a mejoras en la infraestructura, un 30% en maquinarias y equipos, 14% en capacitar su personal, 12% en nuevas tecnologías de producción, 7% en nueva infraestructura y el 5% restante en nuevas sucursales; es decir ninguna de ellas realizó alguna inversión en seguridad de la información, lo cual claramente demuestra la gran vulnerabilidad en la que se encuentra el segmento.

Según el “*barómetro de riesgos*” de la compañía de seguros Allianz (Allianz Global Corporate & Specialty SE, 2018), el riesgo cibernético puede materializarse para una empresa de múltiples y peligrosas formas que se describen a continuación:

Ataques cibernéticos: Violación a la seguridad de la red de la empresa mediante un acceso no autorizado a esta. En los ataques cibernéticos los delincuentes pretenden secuestrar la información, mediante la instalación de un software malicioso o “malware” que amenaza con modificar, alterar, destruir, eliminar, transmitir o registrar la información, generalmente a cambio de una suma de dinero que puede ser en su mayoría en una moneda virtual. (Suramericana, 2015)

Fraude Electrónico: Violación a la seguridad de las cuentas bancarias, sustrayendo una cantidad de dinero o realizando compras por medios electrónicos con los datos de tarjetas de crédito o débito.

Violación de datos: Daño, alteración, distorsión, destrucción o hurto de los activos digitales de las personas o las empresas. (Suramericana, 2015)

Las anteriores situaciones traen grandes consecuencias para la empresa como lo son: extorsiones cibernéticas, pérdidas económicas por fraude, fallo en los sistemas que soportan la operación, interrupción del negocio, pérdida de la reputación, responsabilidad civil por la fuga de información personal de clientes o proveedores, multas y sanciones asociadas al incumplimiento de medidas de seguridad, entre muchas otras situaciones que para el caso de una empresa del segmento Mipyme, puede representar situaciones que ponen en riesgo la continuidad de su negocio (Allianz Global Corporate & Specialty SE, 2018).

La empresa para recuperarse de un crimen cibernético debe acudir a sus utilidades, con el fin de invertir en la reparación de los daños propios y a terceros. Los costos asociados a estos daños pueden implicar, la contratación de un servicio o un personal para reparar o recuperar la información, el pago de indemnizaciones a terceros que hayan sido afectados, además de una inversión en seguridad para evitar futuros eventos. Es por esto que el seguro es una buena herramienta para transferir el riesgo cibernético, pues se convierte en un mecanismo que puede entregar a la Mipyme la capacidad de resiliencia necesaria en un evento de este tipo.

El cibercrimen en Colombia y en sus empresas.

Debido a la creciente preocupación en la última década por el incremento en los delitos cibernéticos, la Policía Nacional de Colombia, crea una subdivisión encargada de vigilar y

atender los casos de crimen cibernético, llamado Centro Cibernético Policial. En el 2017, esta división, publica un informe donde se caracteriza y cuantifica el riesgo en Colombia.

De acuerdo con esta información, los crímenes cibernéticos le han costado al país pérdidas por alrededor de \$1 billón de pesos en 2017, lo que equivale al 0.12% del PIB del mismo año (Banco de la República, Subgerencia de Estudios Económicos., 2018), cifra muy relevante para la economía del país. Las principales regiones donde se producen la mayor cantidad de delitos cibernéticos corresponden a Bogotá, Medellín, Cali, Bucaramanga y Barranquilla, esto debido a que en ellas está el mayor porcentaje de conexión a internet.

Son varias las fuentes que afirman que, en Latinoamérica, los ataques cibernéticos han ido migrando de personas a empresas. Una importante reaseguradora alemana, publicó un reporte llamado "*Los Ciberriesgos y el Seguro*" donde se analizó los cambios en los incidentes cibernéticos, indicando que estos han aumentado en un 38% más entre el 2014 y el 2015 y un 56% de estos hacen referencia a robos de propiedad intelectual en las empresas (Munich RE, 2016). Afirma también que las pequeñas y medianas empresas son las que están siendo objetivo de ciberataques, debido a sus bajos presupuestos y su falta de priorización en las inversiones en seguridad. Por otro lado, Marsh, multinacional corredora de seguros, publica un artículo en 2016 indicando que en las empresas ha crecido en un 4% la preocupación por recibir demandas debido a crímenes cibernéticos. Así mismo en el informe de la Policía Nacional se indica que entre los años 2016 y 2017, se ha presentado una reducción del 35% de los ataques cibernéticos a las personas, pero en caso contrario ha aumentado en un 28% los ataques a las empresas (Centro Cibernético Policial, 2017).

Seguros de riesgo cibernético en Colombia para empresas.

Teniendo en cuenta el panorama del riesgo cibernético en las empresas colombianas, se hace necesario revisar la oferta de seguros vigente enfocada en el segmento.

Actualmente en Colombia, solo tres compañías de seguros, cuentan con ofertas para el riesgo cibernético, Chubb, SBS y Seguros SURA Colombia.

Estas ofertas son de seguros de responsabilidad civil por daños a terceros, donde se ofrecen coberturas por fallas en el tratamiento de datos personales, protección a la reputación, gastos de defensa, pérdidas de activos digitales, interrupción del negocio y en algunos casos extorsión cibernética.

Estas soluciones de aseguramiento, son aún incipientes cuando se habla de daños propios, pues como bien su nombre lo indica, su principal objetivo es cubrir la responsabilidad civil por daños a terceros, por lo tanto, los daños propios de la empresa pasan a un segundo plano y en ninguna de las soluciones de seguros actuales se tiene un cubrimiento de incremento de la seguridad de la información o de contratación de personas para reconstruir la información. Siendo estas últimas dos, los principales gastos en los que las empresas estudiadas invirtieron su dinero como consecuencia del evento cibernético.

Cálculo del impacto del crimen cibernético en las Mipymes.

El seguro de riesgo cibernético es un instrumento de financiación de riesgo para las Mipymes colombianas, debido a que, al exponerse a los riesgos en la web, las pérdidas económicas pueden ser cuantiosas y además puede producirse la interrupción parcial o total de su negocio.

Para realizar el cálculo del bienestar que una Mipyme ganaría cuando experimenta un evento cibernético con la compra de un seguro, se seguirá la metodología planteada en el artículo

de *Kesan et al* (2006) y aplicada posteriormente por *Kuru y Bayraktar* (2017) en el artículo “*The effect of cyber-risk insurance to social welfare*”.

Para efectos de este estudio se tuvo en cuenta datos anónimos de 50 Mipymes en Colombia pertenecientes a varios sectores de la economía, las cuales fueron víctimas de diferentes delitos cibernéticos. Las empresas que se estudiaron no contaban con un seguro contra el riesgo cibernético y en todos los casos experimentaron pérdidas económicas. El formato de la encuesta incluye además de los datos numéricos del evento cibernético, preguntas sobre la actividad de la pyme y el tipo de evento que lo afectó (se puede observar el en anexo 3). Esta encuesta fue divulgada por dos grupos de empresarios a nivel nacional, uno de ellos es conformado por empresarios afiliados a la ANDI del Futuro¹² y otro es un grupo de empresas de todos los tamaños, el cual se formó como una “red social” de apoyo, alianzas y conexiones.

Para el cálculo de las utilidades y el impacto que el seguro tendría en ellas en caso de sufrir un evento cibernético, se tiene en cuenta las variables del estudio que plantea *Kesan (2004)* donde:

I_1^e : *Ingresos en el buen estado de la Pyme* (Sin sufrir un evento cibernético)

I_0^e : *Ingresos en el mal estado de la Pyme* (Sufriendo un evento cibernético)

$L^e = I_1^e - I_0^e$: *Perdidas en un evento cibernético*

s : *Limite economico asegurado*

γ : *Precio por cada peso (COP) asegurado o tasa del seguro*

De acuerdo a lo anterior se tiene que:

γs , corresponde a la prima pagada por el seguro de riesgo cibernético.

¹² La ANDI, (Asociación Nacional de Industriales) tiene una red de emprendedores donde convergen empresas sostenibles, diversas, dinámicas e innovadores.

p , es la probabilidad de tener una pérdida L_e , en el mal estado y en el buen estado, esto ocurriría con una probabilidad de $(1-p)$.

Las empresas generalmente compran un seguro con el fin de transferir sus riesgos y como consecuencia de esta transferencia, se espera una maximización de la utilidad esperada, por lo tanto, el cálculo de esta, es de vital importancia para el desarrollo de la metodología.

La función de utilidad esperada, será entonces la suma de las utilidades correspondientes a los resultados de los dos escenarios posibles, los cuales hacen referencia al buen y al mal estado ponderados por la probabilidad de que cada uno de ellos se produzca.

La utilidad asociada al mal estado será: las ganancias de la empresa sin tener un evento cibernético, menos la prima pagada por el seguro más la cantidad de cobertura comprada así: $U(I_1^e - L^e - \gamma s + s)$. La utilidad asociada al buen estado será: las ganancias de la empresa en el buen estado, menos el gasto en la prima de seguro así: $U(I_1^e - \gamma s)$. De acuerdo a lo anterior y a la definición de la utilidad esperada (EU), la forma que representa la maximización la utilidad de la empresa en el buen y el mal estado es la de von Neumann y Morgenstern:

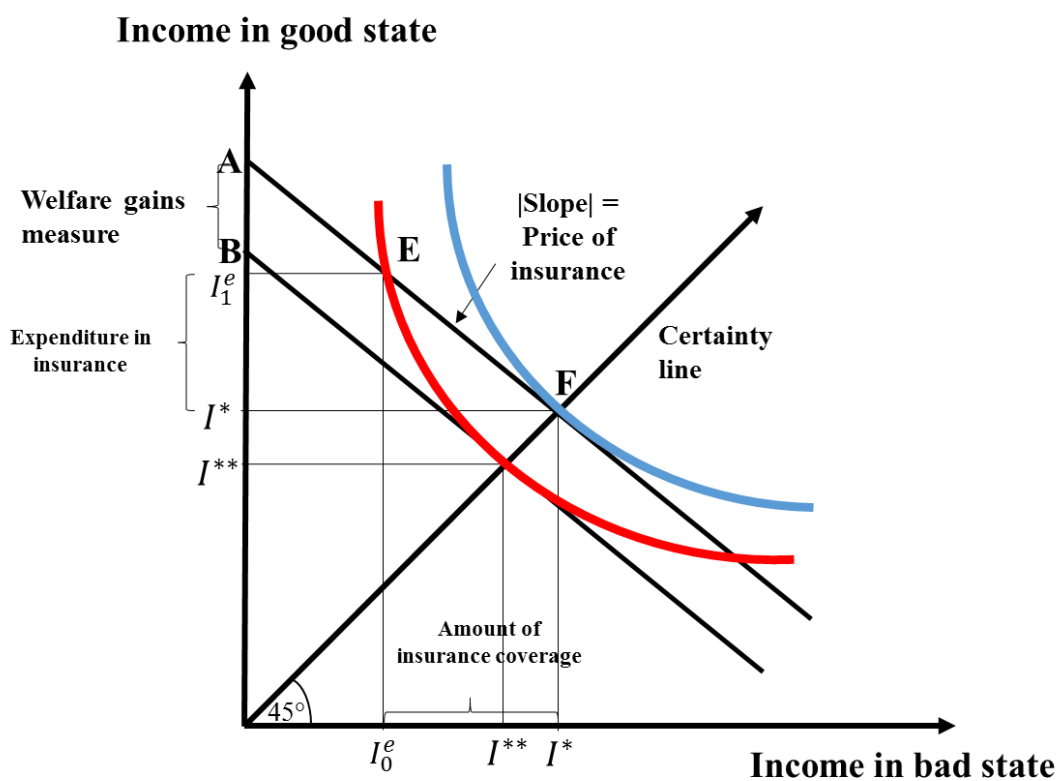
$$EU = pU(I_1^e - L^e - \gamma s + s) + (1 - p)U(I_1^e - \gamma s)$$

La variación del bienestar de una Mipyme para este caso de estudio está relacionada con la posibilidad de que el riesgo cibernético se materialice o no, además de la cantidad de riesgo que la empresa está dispuesta a tomar, es decir su nivel de aversión al riesgo (Jay P. Kesan R. P., 2006).

Para calcular la cantidad de bienestar se analizan dos escenarios: cuando no se tiene contratado ningún seguro y cuando se tiene contratado un seguro. Para representar esta idea se puede ver en la figura 2, como el punto E se refiere al punto inicial, en el cual la Mipyme no

tiene un seguro de riesgo cibernético, y se desplaza hasta el punto F donde la Mipyme está completamente asegurada¹³, a una curva de indiferencia superior, lo que significa mayor bienestar cuando compra el seguro. La cantidad de bienestar ganado se puede observar como la diferencia entre el punto A y el punto B, \overline{AB} .

Figura 2: Explicación grafica de la cantidad de bienestar.



Fuente: Elaboración propia basado en (Jay P. Kesav R. P., 2006)

Para este caso, se supone que el precio de las primas que vamos a usar para el ejercicio, es actuarialmente justo¹⁴, es decir que la compañía de seguros, cobrará una prima de acuerdo con

¹³ Cuando se refiere a que la Mipyme se encuentra completamente asegurada con una prima actuarialmente justa. Es decir que la cantidad de seguro comprada es igual a la pérdida máxima probable.

¹⁴ Prima Actuarialmente Justa: Corresponde a que la prima cobrada por el seguro, es igual a la cantidad de dinero que la compañía espera desembolsar de acuerdo a la medición de probabilidad de ocurrencia de un evento en el mercado.

las probabilidades de pérdida reales, y que será cobrada a todos los clientes de acuerdo a la ley de grandes números y así mismo estará dispuesta a pagar por los eventos que sean reclamados.

Siendo así: $p=\gamma$ y $L^e = s$

Teniendo en cuenta los conceptos anteriores, se sigue una serie de pasos descritos en el anexo 1, para el cálculo de \overline{AB} , como la cantidad de bienestar ganado para las empresas al comprar un seguro.

De acuerdo a la figura 2 se explica que:

La utilidad de A, representada como una curva azul y por la forma $U_a = A: U_a = (1 - p)I_1^e + p(I_0^e)$ para $p > 0$. U_a , se presenta teniendo en cuenta primas actuarialmente justas y representa el contrato ideal para ambas partes. U_b , representado por la curva roja, simboliza el estado en el cual no se está usando ningún seguro de riesgo cibernético. Todos los puntos a lo largo de la línea de 45° (Certainty Line), también llamada línea de presupuesto, muestra todos los puntos donde los dos estados de riqueza son iguales. De acuerdo a la asignación de la eficiencia de Pareto, si el mercado se encuentra en equilibrio, en esta línea ocurrirá la maximización de la utilidad, siendo así se pueden calcular las condiciones de tangencia y se debe poder calcular I^{**} para varios niveles de riesgo. Este cálculo se hace necesario para medir B, que se puede representar como: $I^{**} = B - p \cdot I^{**}$ o $U_b = B: B = (1 + p) \cdot I^{**}$, así la curva que representa a U_b , sube y baja de con distintos niveles de crimen cibernético. Teniendo en cuenta todo lo anterior cuando $I_1^e = I_0^e = I^{**}$, se encuentra el punto donde se maximiza la utilidad cuando no se tiene ningún seguro y cuando $I_1^e = I_0^e = I^*$, es el punto en cual se maximiza la utilidad teniendo un seguro.

Siguiendo la idea anterior, $I_1^e - I^*$, es representado como el gasto en la compra del seguro, es decir la cantidad de dinero pagada por unidad monetaria de cobertura. En resumen, si

no se produce un ataque cibernético, la empresa se podrá mantener en el buen estado (I_1^e), menos el costo que tuvo que pagar por el seguro ($I_1^e - I^*$). En el caso de que se presente un ataque cibernético, la compañía de seguros, pagará a la empresa la diferencia entre el estado habiendo comprado el seguro y el mal estado ($I^* - I_0^e$), por lo tanto el bienestar ganado será la distancia entre A y B (Damla Kuru, 2017).

Para llegar a \overline{AB} , se tomaron en cuenta los siguientes datos de la muestra de las 50 empresas:

$I_0^e = \$ 3.996.030.000$, Corresponde a las utilidades de las 50 Mipymes encuestadas, en el año en el cual experimentaron un evento cibernético,

$I_1^e = \$ 4.368.475.000$, Corresponde a la sumatoria de las utilidades que hubieran tenido estas empresas en caso de no haber experimentado un evento cibernético.

$L^e = \$ 372.445.000$, Corresponde a la sumatoria de las pérdidas económicas que las 50
 $p=\gamma= 0.002, 0.0025, 0.003, 0.0035, 0.004, 0.0045$. Las tarifas por peso colombiano que se pagan en Colombia por el seguro de riesgo cibernético, están entre 2,0‰ y 4,5‰ (por mil). Esto depende ampliamente de varios factores como la compañía aseguradora, el tipo de empresa, es decir la exposición del cliente al riesgo y el monto a asegurar, este último siendo definitivo debido a los cupos que puede asegurar una compañía de seguros en su retención¹⁵. Por lo tanto, se puede decir que las probabilidades de que un ataque ocurra según las tarifas dadas en Colombia, están entre el 0,2% y 0,45%.

Elección del coeficiente de aversión al riesgo:

¹⁵ La retención, es la porción de la prima de seguros y del siniestro que decide asumir la compañía de seguros por su cuenta, sin transferirlo a reaseguro.

Para elegir los coeficientes de aversión al riesgo que se suponen adecuados para la muestra se toma en cuenta, el planteamiento de Holt & Laury, (2002), el cual basa su definición de los valores de referencia de los coeficientes de aversión al riesgo mediante la explicación del riesgo de jugadores a la lotería. Se utiliza esta referencia teniendo en cuenta que la ocurrencia de un evento cibernético, puede asemejarse a los juegos de azar, pues no deja de ser una posibilidad. Por lo tanto la tabla 3 extrae la información que se tendrá en cuenta en este estudio, basado en la tabla 2.

Tabla 2: Coeficientes de aversión al riesgo basado en las decisiones de compra de lotería

Number of safe choices	Range of relative risk aversion for $U(x) = x^{1-r}/(1-r)$	Risk preference classification	Proportion of choices		
			Low real ^a	20x hypothetical	20x real
0-1	$r < -0.95$	highly risk loving	0.01	0.03	0.01
2	$-0.95 < r < -0.49$	very risk loving	0.01	0.04	0.01
3	$-0.49 < r < -0.15$	risk loving	0.06	0.08	0.04
4	$-0.15 < r < 0.15$	risk neutral	0.26	0.29	0.13
5	$0.15 < r < 0.41$	slightly risk averse	0.26	0.16	0.19
6	$0.41 < r < 0.68$	risk averse	0.23	0.25	0.23
7	$0.68 < r < 0.97$	very risk averse	0.13	0.09	0.22
8	$0.97 < r < 1.37$	highly risk averse	0.03	0.03	0.11
9-10	$1.37 < r$	stay in bed	0.01	0.03	0.06

^a Average over first and second decisions.

Fuente: (Holt & Laury, 2002)

Para efectos de este ejercicio se supone que el segmento Mipyme es siempre averso al riesgo en sus diferentes niveles, pues no tiene la capacidad económica de tomar riesgo y no estaría dispuesta exponer su capital en otros asuntos diferentes al desarrollo de su negocio adicionalmente no estaría en capacidad de asumir el costo de los eventos cibernéticos. Es importante tener en cuenta que la actitud de aversión al riesgo es la más común en los

consumidores (Pindyck & Rubinfeld, 2013), pues siempre que se es consciente de un riesgo tiende a evitarse a toda costa. Si bien el riesgo cibernético es aún un terreno desconocido para las Mipymes, se toma como referencia su comportamiento en general frente al riesgo, pues hoy en su mayoría deben comprar un seguro de incendio debido a su aversión al riesgo la cual se manifiesta como el miedo a perder su negocio debido a la materialización de un daño a su infraestructura física. Siendo así, solo se usarán coeficientes de empresas aversas al riesgo en diferentes niveles. Esta selección se hace aleatoria y en promedio entre los rangos estudiados y corresponden a:

$\sigma = 0.2, 0.5, 0.8, 1.2, 1.5$, para los diferentes niveles de riesgo, escogieron los siguientes coeficientes de aversión al riesgo.

En la tabla 3 se muestra la selección de rangos que se tomaran para este caso:

Tabla 3: Coeficientes de aversión al riesgo en la función CRRA y su definición.

Grado de aversión	Rango de Coeficiente	σ Seleccionado
Ligeramente averso al riesgo	$0,15 < A < 0,41$	0,2
Averso al riesgo	$0,41 < A < 0,68$	0,5
Muy averso al riesgo	$0,68 < A < 0,97$	0,8
Altamente averso al riesgo	$0,97 < A < 1,36$	1,2
Aversión extrema al riesgo	$> 1,36$	1,5

Fuente: Elaboración propia basado en (Holt & Laury, 2002)

Este coeficiente es necesario para el cálculo de la EU (utilidad esperada) para la cual se asume la función CRRA de acuerdo a sus características. (Chavez, Milanesi, & Pesce, 2016).

A Partir de los datos mostrados, se calcula la utilidad esperada EU y a partir de estos datos se calcula \overline{AB} .

En la tabla 4 se observan los resultados correspondientes a los cálculos de \overline{AB} , para cada variación de probabilidades de ocurrencia y aversión al riesgo.

Tabla 4: Resultados para 50 empresas

$p = \gamma$	σ	EU	I^{**}	A	B	\overline{AB}
0,002	0,2	\$ 64.433.856,64	\$ 4.367.721.886,88	\$ 4.376.467.060,00	\$ 4.376.457.330,65	\$ 9.729,35
0,002	0,5	\$ 132.177,36	\$ 4.367.713.551,16	\$ 4.376.467.060,00	\$ 4.376.448.978,26	\$ 18.081,74
0,002	0,8	\$ 423,66	\$ 4.367.703.379,14	\$ 4.376.467.060,00	\$ 4.376.438.785,89	\$ 28.274,11
0,002	1,2	\$ (0,05901)	\$ 4.367.689.532,87	\$ 4.376.467.060,00	\$ 4.376.424.911,94	\$ 42.148,06
0,002	1,5	\$ (0,00003)	\$ 4.367.678.930,74	\$ 4.376.467.060,00	\$ 4.376.414.288,60	\$ 52.771,40
0,0025	0,2	\$ 64.431.639,55	\$ 4.367.534.027,20	\$ 4.378.465.075,00	\$ 4.378.452.862,27	\$ 12.212,73
0,0025	0,5	\$ 132.174,48	\$ 4.367.523.199,31	\$ 4.378.465.075,00	\$ 4.378.442.007,31	\$ 23.067,69
0,0025	0,8	\$ 423,66	\$ 4.367.510.490,96	\$ 4.378.465.075,00	\$ 4.378.429.267,18	\$ 35.807,82
0,0025	1,2	\$ (0,05901)	\$ 4.367.493.192,57	\$ 4.378.465.075,00	\$ 4.378.411.925,55	\$ 53.149,45
0,0025	1,5	\$ (0,00003)	\$ 4.367.479.947,43	\$ 4.378.465.075,00	\$ 4.378.398.647,29	\$ 66.427,71
0,003	0,2	\$ 64.429.422,45	\$ 4.367.346.169,14	\$ 4.380.463.090,00	\$ 4.380.448.207,65	\$ 14.882,35
0,003	0,5	\$ 132.171,60	\$ 4.367.332.851,62	\$ 4.380.463.090,00	\$ 4.380.434.850,18	\$ 28.239,82
0,003	0,8	\$ 423,66	\$ 4.367.317.609,59	\$ 4.380.463.090,00	\$ 4.380.419.562,42	\$ 43.527,58
0,003	1,2	\$ (0,05901)	\$ 4.367.296.862,86	\$ 4.380.463.090,00	\$ 4.380.398.753,45	\$ 64.336,55
0,003	1,5	\$ (0,00003)	\$ 4.367.280.977,71	\$ 4.380.463.090,00	\$ 4.380.382.820,64	\$ 80.269,36
0,0035	0,2	\$ 64.427.205,35	\$ 4.367.158.312,70	\$ 4.382.461.105,00	\$ 4.382.443.366,80	\$ 17.738,20
0,0035	0,5	\$ 132.168,72	\$ 4.367.142.508,08	\$ 4.382.461.105,00	\$ 4.382.427.506,86	\$ 33.598,14
0,0035	0,8	\$ 423,65	\$ 4.367.124.735,04	\$ 4.382.461.105,00	\$ 4.382.409.671,62	\$ 51.433,38
0,0035	1,2	\$ (0,05901)	\$ 4.367.100.543,74	\$ 4.382.461.105,00	\$ 4.382.385.395,64	\$ 75.709,36
0,0035	1,5	\$ (0,00003)	\$ 4.367.082.021,59	\$ 4.382.461.105,00	\$ 4.382.366.808,66	\$ 94.296,34
0,004	0,2	\$ 64.424.988,26	\$ 4.366.970.457,88	\$ 4.384.459.120,00	\$ 4.384.438.339,71	\$ 20.780,29
0,004	0,5	\$ 132.165,84	\$ 4.366.952.168,68	\$ 4.384.459.120,00	\$ 4.384.419.977,35	\$ 39.142,65
0,004	0,8	\$ 423,65	\$ 4.366.931.867,31	\$ 4.384.459.120,00	\$ 4.384.399.594,78	\$ 59.525,22
0,004	1,2	\$ (0,05901)	\$ 4.366.904.235,21	\$ 4.384.459.120,00	\$ 4.384.371.852,15	\$ 87.267,85
0,004	1,5	\$ (0,00003)	\$ 4.366.883.079,06	\$ 4.384.459.120,00	\$ 4.384.350.611,38	\$ 108.508,62
0,0045	0,2	\$ 64.422.771,16	\$ 4.366.782.604,67	\$ 4.386.457.135,00	\$ 4.386.433.126,39	\$ 24.008,61
0,0045	0,5	\$ 132.162,96	\$ 4.366.761.833,43	\$ 4.386.457.135,00	\$ 4.386.412.261,68	\$ 44.873,32
0,0045	0,8	\$ 423,64	\$ 4.366.739.006,39	\$ 4.386.457.135,00	\$ 4.386.389.331,92	\$ 67.803,08
0,0045	1,2	\$ (0,05901)	\$ 4.366.707.937,27	\$ 4.386.457.135,00	\$ 4.386.358.122,99	\$ 99.012,01
0,0045	1,5	\$ (0,00003)	\$ 4.366.684.150,13	\$ 4.386.457.135,00	\$ 4.386.334.228,81	\$ 122.906,19

Fuente: elaboración propia.

Análisis y proyección de resultados:

A partir de los datos obtenidos en la tabla 4, se observa que existe una ganancia de bienestar para las empresas que se usaron en la muestra, para todos los escenarios proyectados, esto teniendo en cuenta que el bienestar aumenta, en la medida en que la empresa es más aversa al riesgo y las probabilidades de ocurrencia de un evento cibernético son mayores.

En la medida en que la empresa compraría una mayor cantidad de seguro, es decir teniendo en cuenta una probabilidad igual a la tarifa del seguro $p=\gamma$, se maximiza el bienestar. Si se compara el último resultado que corresponde al bienestar para $p=\gamma= 0,0045$ y un coeficiente de aversión al riesgo $\sigma=1,5$ correspondiente a una empresa extremadamente aversa al riesgo, el bienestar ganado es de \$122.906, lo cual es 12,6 veces mayor que el bienestar ganado para un $p=\gamma= 0,002$ y $\sigma=0,2$ que equivale a una empresa ligeramente aversa al riesgo. A partir de esta comparación se puede decir que la compra del seguro adecuado de acuerdo al riesgo que la empresa esté dispuesta a correr, puede hacer la diferencia en términos de bienestar que la empresa puede esperar recibir en caso de sufrir un evento cibernético.

Estos resultados, concuerdan con los resultados obtenidos en los artículos de referencia, ya que en estos el comportamiento fue similar, a pesar de que los datos de probabilidad de ocurrencia p y los coeficientes de aversión al riesgo σ , fueron significativamente diferentes. El resultado de este análisis, afirma la hipótesis planteada en la cual se ratifica que el seguro para el riesgo cibernético, incrementa el bienestar de una empresa al sufrir un evento de este tipo.

Ejercicio exploratorio de proyección de resultados y análisis del PIB

Para efectos de comparación y teniendo en cuenta que los datos analizados solo representan una muestra del 0,002%, se analizara el impacto que podría tener el bienestar ganado por la compra de un seguro de riesgo cibernético, con respecto al PIB que el segmento aporta al país. Cabe anotar que se proyectan los resultados suponiendo que hipotéticamente todas las Mipymes se comportarían de la misma forma que las 50 empresas encuestadas.

Se puede decir que:

PIB 2017¹⁶(Precios contantes, año base 2015): \$ 835.165.000.000.000

% PIB Mipymes: 28%

Aporte PIB Mipymes: \$ 233.846.200.000.000

Mipymes en Colombia (Dato Aproximado): 2.500.000

PIB per Mipyme (Dato Aproximado): \$ 93.538.480

PIB por 50 Mipymes analizadas (Dato Aproximado): \$ 4.676.924.000

Si el bienestar medido para 50 empresas Mipyme nos arroja un resultado un rango entre: \$9.729,35 y \$122.906,19, haciendo la relación con el PIB total del país para el primer trimestre del 2018:

	Rango inf.	Rango Sup.
Bienestar 50 Mipymes	\$ 9.729	\$ 122.906
Incidencia en PIB 50 Mipymes	0,00021%	0,00263%
Valor Aproximado PIB Mipymes	\$ 486.467.560	\$ 6.145.309.666
Valor Aproximado aporte PIB 2017	\$ 1.737.384.143	\$ 21.947.534.522

¹⁶ Tomado del Boletín de informes económicos del Banco de la Republica del 25 de junio de 2018

Se observa que, de acuerdo con la proyección anterior, los valores de aporte al PIB, si bien en porcentaje parecen pequeños, en valor son significativos para ilustrar el ejercicio mediante el cual, se analiza el seguro como generador de bienestar.

Aseguramiento de las Mipymes.

El bienestar ganado es pequeño comparado con el valor de las pérdidas, pues en porcentaje, esto representa entre el 0,002% y el 0,03% de ellas, de acuerdo a los escenarios planteados lo que indica que, los valores que hoy se están asegurando como pérdidas máximas probables, no son suficientes, o deben ajustarse con el fin de entregar mayor bienestar a las empresas. Esto implica, que para el segmento Mipyme deben reevaluarse las ofertas del mercado de seguros actual. Teniendo en cuenta que las Mipymes en la encuesta realizada para determinar el riesgo cibernético, manifestaron que las pérdidas económicas principales derivadas de un evento cibernético, se debieron a un incremento en los costos de operación por contratación de personal para recuperar o reconstruir la información. Para el caso de las empresas que experimentaron fraude por internet, los costos o gastos del fraude como tal, se incrementaron por la gestión del evento frente a las plataformas transaccionales o bancarias. Sin embargo, manifiestan que aun después de la gestión en algunos casos no pudieron recuperar su dinero, generando así una falta de liquidez que afectó el desarrollo normal de su negocio. Siendo así, se puede concluir que el peor escenario de riesgo aún no se ha materializado, y los valores asegurados, y las primas recolectadas serían insuficientes para soportarlo, además de que un seguro de riesgo cibernético, no podría solo limitarse al cubrimiento de las pérdidas económicas asociadas al cibercrimen, si no que tendría que abarcar también los gastos y costos adicionales que esto representa para la empresa. Esto no es demostrable mediante una teoría económica, pues

el seguro hoy en día solo se extiende a cubrir las pérdidas materiales y la responsabilidad por daños a terceros derivadas de un evento de carácter cibernético.

Para el caso de una Mipyme que no está relacionada con un negocio de tecnología o digital no tiene conocimientos de seguridad de la información, ni invierte en tecnología informática y seguridad, las compañías de seguros en la resignificación del riesgo, debe encontrar la forma de entregar esa capacidad de resiliencia necesaria, mediante la generación de capacidades de autogestión del riesgo. Es decir, formular una oferta de aseguramiento, donde se vuelvan tangibles las primas pagadas por la empresa, ofreciendo no solo aseguramiento si no una oferta integral que incluya servicios de implementación de esquemas basados en seguridad de la información, donde a su vez garantice a la empresa una disminución en la vulnerabilidad al sufrir cualquier incidente cibernético. Además de entregarle herramientas de prevención y protección en el día a día, para prevenir y mitigar las pérdidas que se deriven de reclamaciones de terceros.

Conclusiones

El riesgo cibernético es aún un riesgo de difícil cuantificación para las compañías aseguradoras, esto indica que aún no se tienen las herramientas, la historia, y el mercado suficiente para disponer de una cuantificación completa de este, con el fin de entregar al cliente una oferta de aseguramiento que le permita financiar su riesgo de manera adecuada.

Se concluye entonces a partir del desarrollo de la metodología que el seguro de riesgo cibernético, si aporta a la protección de las utilidades de las Mipymes. Sin embargo, es importante tener en cuenta que la financiación de riesgos para el caso de las Mipymes es aún un desafío para el mercado asegurador colombiano, pues si bien son un segmento poderoso económicamente, sus inversiones en la actualidad están enfocadas en crecer, mejorando su negocio físicamente, comprando maquinaria y capacitando su personal. La inversión en aseguramiento aun es poca y en su mayoría se realiza por obligación, debido al cumplimiento de un deber, un contrato o asociado a un crédito bancario (Suramericana, 2018).

Es importante tener en cuenta que la dificultad principal encontrada al analizar el mercado de las Mipymes, es la informalidad de la información, no se tienen datos 100% exactos, lo que hace que los datos recolectados sean aproximados. La falta de datos que se encontró es atribuida principalmente a que algunas de las transacciones que realizan no cuentan con soporte oficial (factura) y son reemplazados con vales de caja menor. El formato de la encuesta utilizada se detalla en el anexo 2.

Referencias

- ACOPI. (2018). *Encuesta de desempeño empresarial 1er trimestre de 2018*. Barranquilla: Equipo de estudios económicos. Recuperado el 1 de Junio de 2018, de <http://acopi.org.co/ENCUESTA-DE-DESEMPE%C3%91O-EMPRESARIAL-RESULTADOS-2018.pdf>
- Allianz Global Corporate & Specialty SE. (2018). *Allianz Risk Barometer*. Allianz Group. Munich: Allianz Global Corporate & Specialty SE.
- AON Risk Solutions. (2017). *Global Risk Management Survey*. New York: Aon plc 2017. Recuperado el 11 de Abril de 2018, de <http://www.aon.com/2017-global-risk-management-survey/pdfs/2017-Aon-Global-Risk-Management-Survey-Full-Report-062617.pdf>
- Banco de la República, Subgerencia de Estudios Económicos. (2018). *Boletín de indicadores económicos*.
- Centro Cibernético Policial. (2017). *Amenazas del cibecrimen en Colombia 2016 - 2017*. Bogotá: Dirección de investigación criminal e INTERPOL.
- Chavez, E. S., Milanesi, G., & Pesce, G. (2016). FUNCIONES DE UTILIDAD Y ESTIMACIÓN DE LA AVERSIÓN AL RIESGO: REVISIÓN DE LA LITERATURA. *Escritos Contables y de Administración*, 7(2), 97 a 118.
- Christian Biener, M. E. (2015). *Insurability of Cyber Risk: An Empirical Analysis*. Working Paper on Finance, University of St. Gallen, School of Finance, St. Gallen. Recuperado el 4 de Junio de 2018
- Damla Kuru, S. B. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime*, 24, 329-346.

Eling, M., & Schnell, W. (17 de Septiembre de 2016). What do we know about cyber risk and ciber risk insurance. *The Journal of Risk Finance*, 17(5), 474 - 490. doi:10.1108/JRF-092016-0122

Fasecolda. (12 de 07 de 2018). www.fasecolda.com.co. Obtenido de Fasecolda:

<http://www.fasecolda.com/index.php/servicios/directorio/sociedades-corredoras-de-reaseguros/guy-carpenter-colombia-corredores-de-reaseguros-ltda/>

Grinols, E., & Kar -Yiu. (1991). An Exact Measure of Welfare Change. *The Canadian Journal of Economics /Revue Canidienne D'Economique*, 24(2), 428 - 449. doi:10.2307/135632

Guy Carpenter & Company, LLC. (2015). A Clearing View of Emerging Risk. *Emerging Risk Report*, 7 a 44.

Holt, C., & Laury, S. (2002). Risk Aversion and Incentive Effects. *The American Economic Review*, 92(5), 1645 -1654. Obtenido de [http://community.middlebury.edu/~jcarpent/EC499/Holt%20and%20Laury%20\(2002\)%20AER.pdf](http://community.middlebury.edu/~jcarpent/EC499/Holt%20and%20Laury%20(2002)%20AER.pdf)

Jay P. Kesan, R. M. (2004). *The Economic Case for Cyberinsurance*. Illinois: Illinois Law and Economics Working Papers Series.

Jay P. Kesan, R. P. (2006). *Cyberinsurance as a market-based solution to the problem of cybersecurity - A case study*. University of Illinois at Urbana-Champaign. National Center for Supercomputing Applications (NCSA).

Martin Eling, W. S. (Noviembre de 2016). Ten Key Questions on Cyber Risk and Cyber Risk Insurance. (F. Sommerrock, Ed.) *The Geneva Asociation*, 3-88. Obtenido de https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf

- Munich RE. (2016). *Los ciberrriesgos y el seguro*. Munich.
- Pindyck, R., & Rubinfeld, D. (2013). *Microeconomia* (8° Edicion ed.). Madrid, Rivera del Loira, España: Pearson Educación S.A.
- Ponemon Institute LLC & AON. (2017). *2017 Europe, Middle East & Africa Cyber Risk Transfer Comparison Report*. New York: Ponemon Institute Reserch.
- Shackelford, S. J. (2017). The Law of Cyber Peace. *Chicago Journal of International Law*, 18(1). Obtenido de <https://chicagounbound.uchicago.edu/cjil/vol18/iss1/1>
- Suramericana. (1 de Octubre de 2015). Seguro de proteccion digital global. Medellin, Antioquia, Colombia. Obtenido de <https://www.segurossura.com.co/Paginas/empresas/responsabilidad-civil/proteccion-digital.aspx#p-d-g>
- The Economist Intelligence Unit. (2017). *Europe economy: Wanna Cry ransomware: exposing our cyber-vulnerabilities*. The Economist Intelligence Unit. Recuperado el 2 de Abril de 2018, de http://ezproxy.eafit.edu.co:2273/index.asp?layout=VWArticleVW3&article_id=1165466 300
- Vasseur, J. P., & A, J. A. (2018). Estimación del índice de aversión al riesgo utilizando la función CRRA. *Espacios*, 39(13), 29. Obtenido de <http://www.revistaespacios.com/a18v39n13/a18v39n13p29.pdf>
- World Economic Forum. (2018). *The Global Risk Report 2018*. Geneva. Recuperado el 10 de Abril de 2018, de http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Anexo 1

Paso a paso de la metodología desarrollada.

Se seguirá una serie de pasos para medir el bienestar ganado representado como \overline{AB} , teniendo en cuenta la aplicación planteada por *Kesan (2004)* en su artículo “*The Economic Case for Cyberinsurance*”.

Paso 1: recolectar los datos de I_1^e (*en el buen estado*) y I_0^e (*en el mal estado*)

Se calcula I_1^e como:

$$I_1^e = I_0^e + L^e$$

Paso 2: encontrar la probabilidad de ocurrencia de un ataque cibernético p . Para este caso, se asume que las primas calculadas son actuarialmente justas y que $p=\gamma$.

Paso 3: se asume una función de utilidad que represente al riesgo, en este caso se supone la función CRRA, también llamada función isoelastica, la cual es elegida también en varios artículos de referencia, debido a que es una función simple, que permite la modelación del comportamiento de consumidores aversos, neutrales y propensos al riesgo (Vasseur & A, 2018):

$$U(I) = \begin{cases} \frac{I^{1-\sigma}}{1-\sigma}, & \text{cuando } \sigma > 0, \quad \sigma \neq 1 \\ \text{Log}(I), & \text{cuando } \sigma = 1 \end{cases}$$

Por lo tanto:

$$EU = p \frac{I_0^{1-\sigma}}{1-\sigma} + (1-p) \frac{I_1^{1-\sigma}}{1-\sigma}, \text{ cuando } \sigma > 0, \sigma \neq 1$$

$$EU = p \cdot \ln(I_0^e) + (1-p) \cdot \ln(I_1^e)$$

Paso 4: se procede al cálculo de I^{**} , que corresponde al punto en el cual ocurre la maximización de la utilidad (ver figura 2).

El punto A, se encuentra aplicando la siguiente función:

$$A = I_1^e + p \cdot I_0^e$$

La línea de 45°, es llamada línea de presupuesto, es decir que la maximización ocurre cuando esta línea es tangente a B, y este punto es I^{**17} .

Se debe calcular un I^{**} , para cada coeficiente de aversión al riesgo.

Paso 5: se calcula B, que hace referencia al punto en el cual las Mipyme no tienen seguro de riesgo cibernético, y se resta de A. (ver figura 2 para explicación gráfica). Esto equivale al bienestar ganado para los diferentes niveles de aversión al riesgo y las diferentes opciones de aseguramiento.

Para el cálculo de B, se utiliza la siguiente ecuación:

$$B = (1 - p) \cdot I^{**}$$

¹⁷ Se debe calcular un I^{**} para cada coeficiente de aversión al riesgo, despejando de la ecuación de la Utilidad Esperada EU, suponiendo que $I_1^e = I_0^e = I^{**}$.

Anexo 2

Otros Resultados

Se anexan otros resultados del análisis de 3 empresas de las muestras escogidas aleatoriamente:

Tabla 3: Empresa 2. Empresa de inversiones para extranjeros.

Evento: Ataque Cibernético

$$I_1^e = \$ 41.000.000,00$$

$$I_0^e = \$ 40.000.000,00$$

$$Le = \$ 1.000.000,00$$

$p = \gamma$	σ	<i>EU</i>	<i>I**</i>	<i>A</i>	<i>B</i>	\overline{AB}
0,002	0,2	\$ 1.538.580,09	\$ 40.997.979,52	\$ 41.080.000,00	\$ 41.079.975,48	\$ 24,52
0,002	0,5	\$ 12.805,93	\$ 40.997.987,68	\$ 41.080.000,00	\$ 41.079.983,65	\$ 16,35
0,002	0,8	\$ 166,54	\$ 40.997.980,24	\$ 41.080.000,00	\$ 41.079.976,20	\$ 23,80
0,002	1,2	\$ (0,15011)	\$ 40.997.970,26	\$ 41.080.000,00	\$ 41.079.966,20	\$ 33,80
0,002	1,5	\$ (0,00031)	\$ 40.997.962,73	\$ 41.080.000,00	\$ 41.079.958,66	\$ 41,34
0,0025	0,2	\$ 1.538.565,04	\$ 40.997.478,29	\$ 41.100.000,00	\$ 41.099.971,99	\$ 28,01
0,0025	0,5	\$ 12.805,86	\$ 40.997.484,61	\$ 41.100.000,00	\$ 41.099.978,32	\$ 21,68
0,0025	0,8	\$ 166,54	\$ 40.997.475,31	\$ 41.100.000,00	\$ 41.099.969,00	\$ 31,00
0,0025	1,2	\$ (0,15011)	\$ 40.997.462,84	\$ 41.100.000,00	\$ 41.099.956,50	\$ 43,50
0,0025	1,5	\$ (0,00031)	\$ 40.997.453,44	\$ 41.100.000,00	\$ 41.099.947,07	\$ 52,93
0,003	0,2	\$ 1.538.549,99	\$ 40.996.977,07	\$ 41.120.000,00	\$ 41.119.968,00	\$ 32,00
0,003	0,5	\$ 12.805,78	\$ 40.996.981,54	\$ 41.120.000,00	\$ 41.119.972,48	\$ 27,52
0,003	0,8	\$ 166,54	\$ 40.996.970,39	\$ 41.120.000,00	\$ 41.119.961,30	\$ 38,70
0,003	1,2	\$ (0,15011)	\$ 40.996.955,43	\$ 41.120.000,00	\$ 41.119.946,30	\$ 53,70
0,003	1,5	\$ (0,00031)	\$ 40.996.944,15	\$ 41.120.000,00	\$ 41.119.934,99	\$ 65,01
0,0035	0,2	\$ 1.538.534,95	\$ 40.996.475,85	\$ 41.140.000,00	\$ 41.139.963,51	\$ 36,49
0,0035	0,5	\$ 12.805,70	\$ 40.996.478,47	\$ 41.140.000,00	\$ 41.139.966,14	\$ 33,86
0,0035	0,8	\$ 166,54	\$ 40.996.465,47	\$ 41.140.000,00	\$ 41.139.953,10	\$ 46,90
0,0035	1,2	\$ (0,15011)	\$ 40.996.448,03	\$ 41.140.000,00	\$ 41.139.935,60	\$ 64,40
0,0035	1,5	\$ (0,00031)	\$ 40.996.434,88	\$ 41.140.000,00	\$ 41.139.922,40	\$ 77,60
0,004	0,2	\$ 1.538.519,90	\$ 40.995.974,62	\$ 41.160.000,00	\$ 41.159.958,52	\$ 41,48
0,004	0,5	\$ 12.805,62	\$ 40.995.975,41	\$ 41.160.000,00	\$ 41.159.959,31	\$ 40,69
0,004	0,8	\$ 166,54	\$ 40.995.960,55	\$ 41.160.000,00	\$ 41.159.944,40	\$ 55,60
0,004	1,2	\$ (0,15011)	\$ 40.995.940,64	\$ 41.160.000,00	\$ 41.159.924,40	\$ 75,60
0,004	1,5	\$ (0,00031)	\$ 40.995.925,61	\$ 41.160.000,00	\$ 41.159.909,32	\$ 90,68
0,0045	0,2	\$ 1.538.504,85	\$ 40.995.473,40	\$ 41.180.000,00	\$ 41.179.953,03	\$ 46,97
0,0045	0,5	\$ 12.805,54	\$ 40.995.472,35	\$ 41.180.000,00	\$ 41.179.951,97	\$ 48,03
0,0045	0,8	\$ 166,54	\$ 40.995.455,65	\$ 41.180.000,00	\$ 41.179.935,20	\$ 64,80
0,0045	1,2	\$ (0,15011)	\$ 40.995.433,25	\$ 41.180.000,00	\$ 41.179.912,70	\$ 87,30
0,0045	1,5	\$ (0,00031)	\$ 40.995.416,36	\$ 41.180.000,00	\$ 41.179.895,73	\$ 104,27

Tabla 4: Empresa 5. Empresa de Manufactura de bienes de acero y madera.

Evento: Pérdida de información

$$I_1^e = \$ 230.150.000,00$$

$$I_0^e = \$ 230.000.000,00$$

$$L_e = \$ 150.000,00$$

$p = \gamma$	σ	EU	I^{**}	A	B	\overline{AB}
0,002	0,2	\$ 6.116.716,38	\$ 230.149.612,62	\$ 230.610.000,00	\$ 230.609.911,84	\$ 88,16
0,002	0,5	\$ 30.341,37	\$ 230.149.699,95	\$ 230.610.000,00	\$ 230.609.999,35	\$ 0,65
0,002	0,8	\$ 235,16	\$ 230.149.699,92	\$ 230.610.000,00	\$ 230.609.999,32	\$ 0,68
0,002	1,2	\$ (0,10631)	\$ 230.149.699,88	\$ 230.610.000,00	\$ 230.609.999,28	\$ 0,72
0,002	1,5	\$ (0,00013)	\$ 230.149.699,85	\$ 230.610.000,00	\$ 230.609.999,25	\$ 0,75
0,0025	0,2	\$ 6.116.714,78	\$ 230.149.537,61	\$ 230.725.000,00	\$ 230.724.911,45	\$ 88,55
0,0025	0,5	\$ 30.341,37	\$ 230.149.624,94	\$ 230.725.000,00	\$ 230.724.999,00	\$ 1,00
0,0025	0,8	\$ 235,16	\$ 230.149.624,90	\$ 230.725.000,00	\$ 230.724.998,96	\$ 1,04
0,0025	1,2	\$ (0,10631)	\$ 230.149.624,85	\$ 230.725.000,00	\$ 230.724.998,92	\$ 1,08
0,0025	1,5	\$ (0,00013)	\$ 230.149.624,82	\$ 230.725.000,00	\$ 230.724.998,88	\$ 1,12
0,003	0,2	\$ 6.116.713,19	\$ 230.149.462,61	\$ 230.840.000,00	\$ 230.839.910,99	\$ 89,01
0,003	0,5	\$ 30.341,36	\$ 230.149.549,93	\$ 230.840.000,00	\$ 230.839.998,58	\$ 1,42
0,003	0,8	\$ 235,16	\$ 230.149.549,88	\$ 230.840.000,00	\$ 230.839.998,53	\$ 1,47
0,003	1,2	\$ (0,10631)	\$ 230.149.549,82	\$ 230.840.000,00	\$ 230.839.998,47	\$ 1,53
0,003	1,5	\$ (0,00013)	\$ 230.149.549,78	\$ 230.840.000,00	\$ 230.839.998,43	\$ 1,57
0,0035	0,2	\$ 6.116.711,59	\$ 230.149.387,60	\$ 230.955.000,00	\$ 230.954.910,46	\$ 89,54
0,0035	0,5	\$ 30.341,36	\$ 230.149.474,91	\$ 230.955.000,00	\$ 230.954.998,08	\$ 1,92
0,0035	0,8	\$ 235,16	\$ 230.149.474,86	\$ 230.955.000,00	\$ 230.954.998,03	\$ 1,97
0,0035	1,2	\$ (0,10631)	\$ 230.149.474,80	\$ 230.955.000,00	\$ 230.954.997,96	\$ 2,04
0,0035	1,5	\$ (0,00013)	\$ 230.149.474,74	\$ 230.955.000,00	\$ 230.954.997,91	\$ 2,09
0,004	0,2	\$ 6.116.710,00	\$ 230.149.312,60	\$ 231.070.000,00	\$ 231.069.909,85	\$ 90,15
0,004	0,5	\$ 30.341,35	\$ 230.149.399,90	\$ 231.070.000,00	\$ 231.069.997,50	\$ 2,50
0,004	0,8	\$ 235,16	\$ 230.149.399,84	\$ 231.070.000,00	\$ 231.069.997,44	\$ 2,56
0,004	1,2	\$ (0,10631)	\$ 230.149.399,77	\$ 231.070.000,00	\$ 231.069.997,37	\$ 2,63
0,004	1,5	\$ (0,00013)	\$ 230.149.399,71	\$ 231.070.000,00	\$ 231.069.997,31	\$ 2,69
0,0045	0,2	\$ 6.116.708,40	\$ 230.149.237,59	\$ 231.185.000,00	\$ 231.184.909,16	\$ 90,84
0,0045	0,5	\$ 30.341,35	\$ 230.149.324,89	\$ 231.185.000,00	\$ 231.184.996,85	\$ 3,15
0,0045	0,8	\$ 235,16	\$ 230.149.324,82	\$ 231.185.000,00	\$ 231.184.996,79	\$ 3,21
0,0045	1,2	\$ (0,10631)	\$ 230.149.324,74	\$ 231.185.000,00	\$ 231.184.996,70	\$ 3,30
0,0045	1,5	\$ (0,00013)	\$ 230.149.324,67	\$ 231.185.000,00	\$ 231.184.996,63	\$ 3,37

Tabla 5: Empresa 20. Empresa de hotelería y turismo ecológico.

Evento: Virus o ataque cibernético.

$$I_1^e = \$ 117.700.000,00$$

$$I_0^e = \$ 85.000.000,00$$

$$Le = \$ 32.700.000,00$$

$p = \gamma$	σ	<i>EU</i>		<i>I**</i>		<i>A</i>		<i>B</i>		<i>AB</i>	
0,002	0,2	\$	3.575.460,74	\$	117.632.502,63	\$	117.870.000,00	\$	117.867.767,63	\$	2.232,37
0,002	0,5	\$	21.691,41	\$	117.629.300,61	\$	117.870.000,00	\$	117.864.559,21	\$	5.440,79
0,002	0,8	\$	205,62	\$	117.625.839,52	\$	117.870.000,00	\$	117.861.091,19	\$	8.908,81
0,002	1,2	\$	(0,12158)	\$	117.620.863,23	\$	117.870.000,00	\$	117.856.104,96	\$	13.895,04
0,002	1,5	\$	(0,00018)	\$	117.616.837,13	\$	117.870.000,00	\$	117.852.070,81	\$	17.929,19
0,0025	0,2	\$	3.575.050,72	\$	117.615.640,66	\$	117.912.500,00	\$	117.909.679,77	\$	2.820,23
0,0025	0,5	\$	21.689,78	\$	117.611.629,08	\$	117.912.500,00	\$	117.905.658,15	\$	6.841,85
0,0025	0,8	\$	205,62	\$	117.607.305,24	\$	117.912.500,00	\$	117.901.323,50	\$	11.176,50
0,0025	1,2	\$	(0,12159)	\$	117.601.089,02	\$	117.912.500,00	\$	117.895.091,74	\$	17.408,26
0,0025	1,5	\$	(0,00018)	\$	117.596.060,19	\$	117.912.500,00	\$	117.890.050,34	\$	22.449,66
0,003	0,2	\$	3.574.640,70	\$	117.598.779,18	\$	117.955.000,00	\$	117.951.575,52	\$	3.424,48
0,003	0,5	\$	21.688,15	\$	117.593.958,88	\$	117.955.000,00	\$	117.946.740,76	\$	8.259,24
0,003	0,8	\$	205,61	\$	117.588.773,29	\$	117.955.000,00	\$	117.941.539,61	\$	13.460,39
0,003	1,2	\$	(0,12159)	\$	117.581.318,80	\$	117.955.000,00	\$	117.934.062,75	\$	20.937,25
0,003	1,5	\$	(0,00018)	\$	117.575.288,75	\$	117.955.000,00	\$	117.928.014,62	\$	26.985,38
0,0035	0,2	\$	3.574.230,67	\$	117.581.918,19	\$	117.997.500,00	\$	117.993.454,90	\$	4.045,10
0,0035	0,5	\$	21.686,52	\$	117.576.290,01	\$	117.997.500,00	\$	117.987.807,02	\$	9.692,98
0,0035	0,8	\$	205,60	\$	117.570.243,69	\$	117.997.500,00	\$	117.981.739,54	\$	15.760,46
0,0035	1,2	\$	(0,12160)	\$	117.561.552,56	\$	117.997.500,00	\$	117.973.017,99	\$	24.482,01
0,0035	1,5	\$	(0,00018)	\$	117.554.522,81	\$	117.997.500,00	\$	117.965.963,64	\$	31.536,36
0,004	0,2	\$	3.573.820,65	\$	117.565.057,67	\$	118.040.000,00	\$	118.035.317,90	\$	4.682,10
0,004	0,5	\$	21.684,89	\$	117.558.622,46	\$	118.040.000,00	\$	118.028.856,95	\$	11.143,05
0,004	0,8	\$	205,60	\$	117.551.716,42	\$	118.040.000,00	\$	118.021.923,28	\$	18.076,72
0,004	1,2	\$	(0,12160)	\$	117.541.790,31	\$	118.040.000,00	\$	118.011.957,47	\$	28.042,53
0,004	1,5	\$	(0,00018)	\$	117.533.762,38	\$	118.040.000,00	\$	118.003.897,43	\$	36.102,57
0,0045	0,2	\$	3.573.410,63	\$	117.548.197,64	\$	118.082.500,00	\$	118.077.164,53	\$	5.335,47
0,0045	0,5	\$	21.683,26	\$	117.540.956,24	\$	118.082.500,00	\$	118.069.890,54	\$	12.609,46
0,0045	0,8	\$	205,59	\$	117.533.191,48	\$	118.082.500,00	\$	118.062.090,84	\$	20.409,16
0,0045	1,2	\$	(0,12160)	\$	117.522.032,05	\$	118.082.500,00	\$	118.050.881,19	\$	31.618,81
0,0045	1,5	\$	(0,00018)	\$	117.513.007,44	\$	118.082.500,00	\$	118.041.815,97	\$	40.684,03

Anexo 3

Formato de la encuesta:

La encuesta fue realizada a través de google forms.

Imagen 1: Pagina 1 Encuesta.

28/6/2018

Crimen cibernético o robo o pérdida de información en pymes.

Crimen cibernético o robo o pérdida de información en pymes.

Esta encuesta es para un trabajo investigativo, para optar al título de Magister en economía de la universidad Eafit. sus respuestas son confidenciales y serán tabuladas, nunca se mostrarán de forma individual. Solo debe responder a esta encuesta si ha tenido un evento de crimen cibernético.

*Required

1. ¿Qué productos o servicios presta su empresa? *

2. ¿Cuántos son sus ingresos al año? *

3. ¿Cuánto le costó reparar las pérdidas o daños causados por el ataque cibernético o la pérdida de información? *

4. ¿Qué evento sufrió? *

Mark only one oval.

Pérdida de información

Robo de cuentas

Robo de Información

Secuestro de Información

Virus o ataque cibernético

Fraude por internet

Other: _____

5. ¿Cuántas son sus utilidades al año? *

6. Ciudad *

Imagen 2: Pagina 2 Encuesta.

28/6/2018

Crimen cibernetico o robo o pérdida de información en pymes.

7. ¿Tenia seguro de riesgo cibernetico? **Mark only one oval.* Sí No**8. ¿En que gastos incurrió debido a la perdida?**

Powered by
 Google Forms